POSTAL SERVICE

POSTAGE FEE APPARATUS

| POSTAGE FEE UNIT GENERATOR | 12 |
| ACCOUNTING UNIT | 11 / 15 |

1

| MEMORY | 14 |

INSPECTION UNIT 13

FRANKING APPARATUS

CENTRAL UNIT

23	FEE MODULE
24	CRYPTO GRAPHIC MODULE
21 / 25	PRINT CONTROL MODULE

2

| 22 | PRINTER |

13 3

| INSPECTION UNIT |

MAIL-CARRYING SERVICE

Fig. 1

82   81   84   83

| SENDER FIELD | | DATE STAMP | FEE STAMP |

| ADDRESS FIELD |

8

| LABEL | 85

MAILPIECE

Fig. 2

$$([acc]^P) \leftarrow \text{INSPECT}\ ([u_1, u_2, I]^S, [I]^P)$$

41

USER S   POSTAGE FEE APPARATUS P

$$w_1, w_2 \in_R \mathbb{Z}_q;$$
$$a \leftarrow g_1^{w1}\, g_2^{w2} \bmod p$$

$\xrightarrow{\ a\ }$

$c \in_R \mathbb{Z}_q^*$ 42

$\xleftarrow{\ c\ }$

$$r_1 \leftarrow cu_1 + w_1 \bmod q$$
$$r_2 \leftarrow cu_2 + w_2 \bmod q$$

$\xrightarrow{\ r_1, r_2\ }$ 44

$$acc \equiv (g_1^{r1}\, g_2^{r2} \stackrel{?}{=} h^c a \ (\bmod\ p))$$

43

Fig. 3

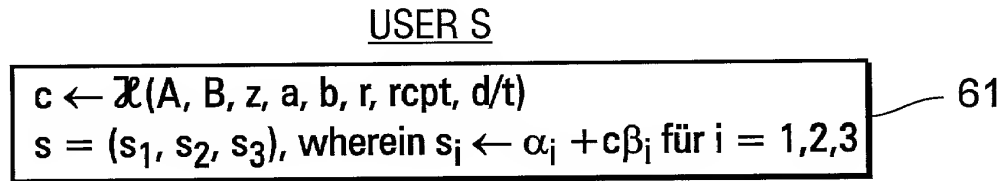$$(s) \leftarrow \text{indicium}\ (A, B, \alpha, \beta, (z, a, b, r), rcpt, d/t)$$

USER S

$$c \leftarrow \mathcal{H}(A, B, z, a, b, r, rcpt, d/t)$$
$$s = (s_1, s_2, s_3),\ \text{wherein}\ s_i \leftarrow \alpha_i + c\beta_i \ \text{für}\ i = 1,2,3$$

61

Fig. 5

$$(u_1, u_2) \quad \text{IDENTIFY DS}\ (c1, s1, c2, s2)$$

INSPECTION UNIT

$$u_1 \leftarrow \frac{s_{11}(c_2 - 1) + s_{21}(1 - c_1)}{s_{13}(c_2 - 1) + s_{23}(1 - c_1)} \bmod q$$

$$u_2 \leftarrow \frac{s_{12}(c_2 - 1) + s_{22}(1 - c_1)}{s_{13}(c_2 - 1) + s_{23}(1 - c_1)} \bmod q$$

71

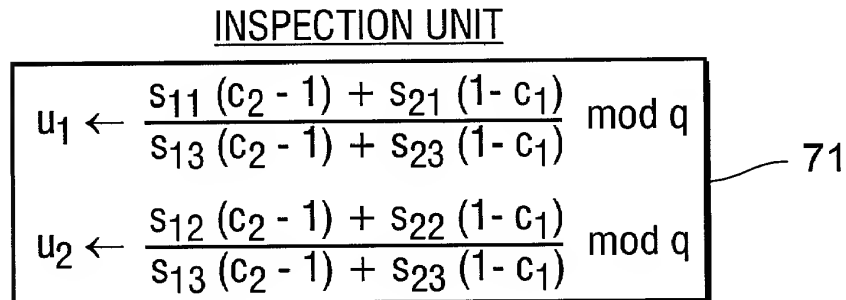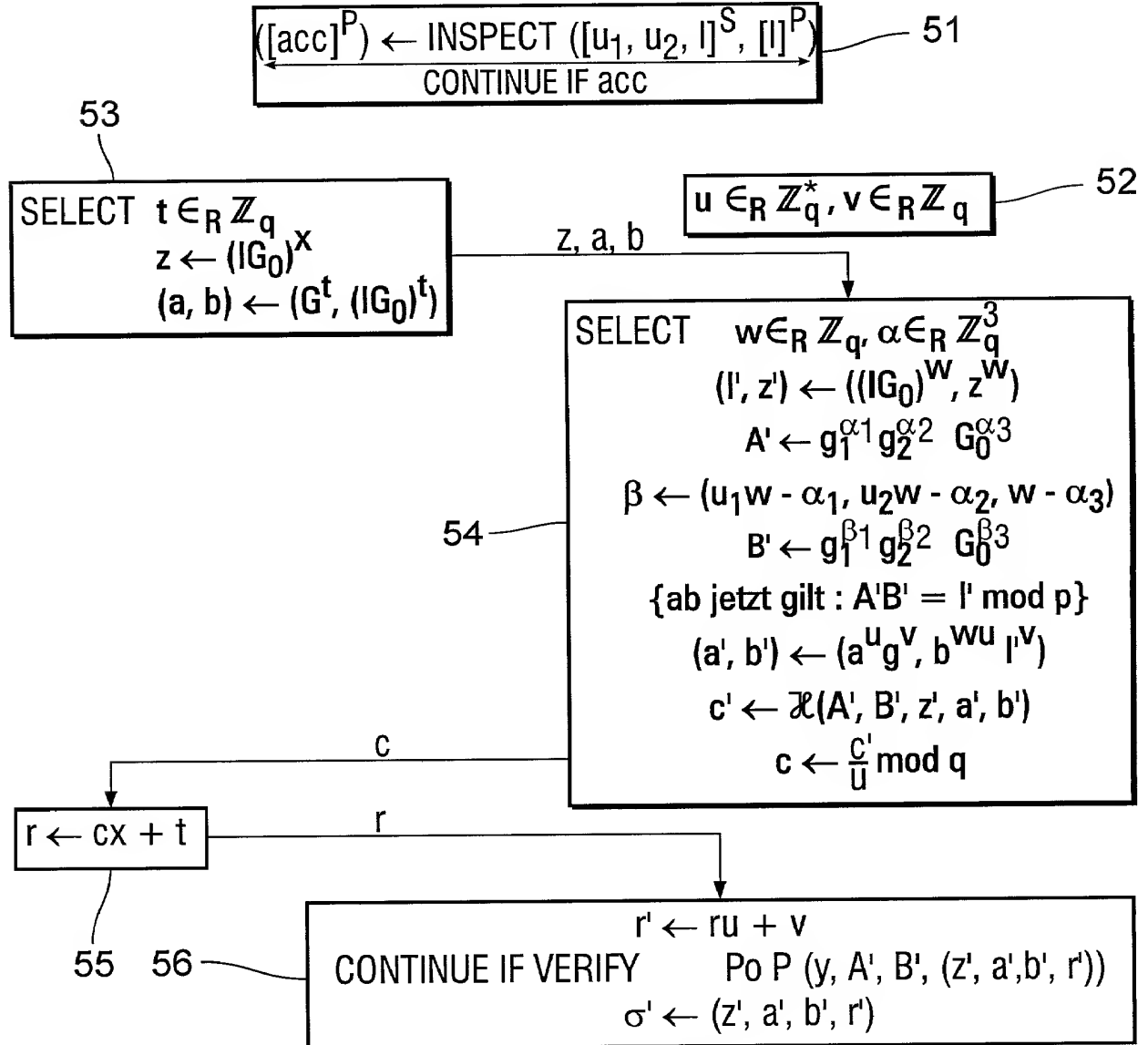**Fig. 6**

$$([A', B', \alpha, \beta, \sigma']^S) \leftarrow \text{DOWNLOAD} ([u_1, u_2, y, l], [x, l]^P)$$

POSTAGE FEE APPARATUS P   USER S

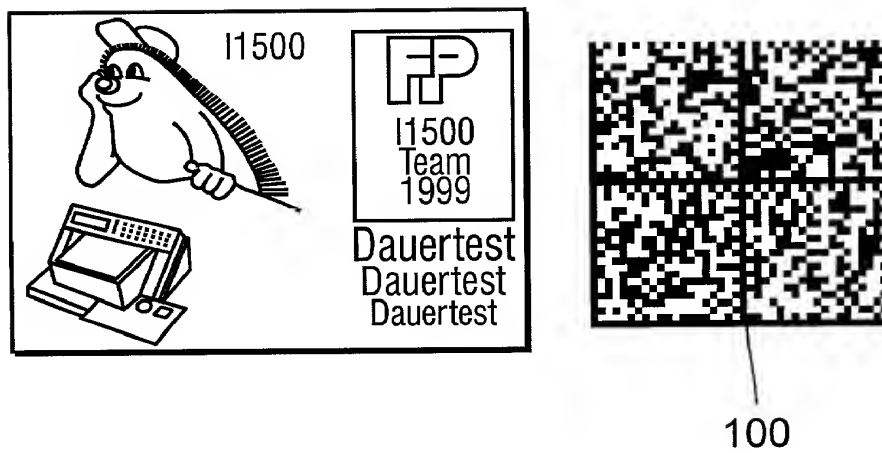$$([acc]^P) \leftarrow \text{INSPECT} ([u_1, u_2, l]^S, [l]^P)$$
CONTINUE IF acc — 51

53

SELECT $t \in_R \mathbb{Z}_q$
$z \leftarrow (lG_0)^x$
$(a, b) \leftarrow (G^t, (lG_0)^t)$

z, a, b

$u \in_R \mathbb{Z}_q^*, v \in_R \mathbb{Z}_q$ — 52

SELECT $w \in_R \mathbb{Z}_q, \alpha \in_R \mathbb{Z}_q^3$
$(l', z') \leftarrow ((lG_0)^w, z^w)$
$A' \leftarrow g_1^{\alpha_1} g_2^{\alpha_2} G_0^{\alpha_3}$
$\beta \leftarrow (u_1 w - \alpha_1, u_2 w - \alpha_2, w - \alpha_3)$
$B' \leftarrow g_1^{\beta_1} g_2^{\beta_2} G_0^{\beta_3}$
{ab jetzt gilt : $A'B' = l' \bmod p$}
$(a', b') \leftarrow (a^u g^v, b^{wu} l'^v)$
$c' \leftarrow \mathcal{H}(A', B', z', a', b')$
$c \leftarrow \frac{c'}{u} \bmod q$

54

c

$r \leftarrow cx + t$

r

55   56

$r' \leftarrow ru + v$
CONTINUE IF VERIFY   Po P $(y, A', B', (z', a', b', r'))$
$\sigma' \leftarrow (z', a', b', r')$

Fig. 4

I1500

FP
I1500
Team
1999
Dauertest
Dauertest
Dauertest

100

Fig. 7